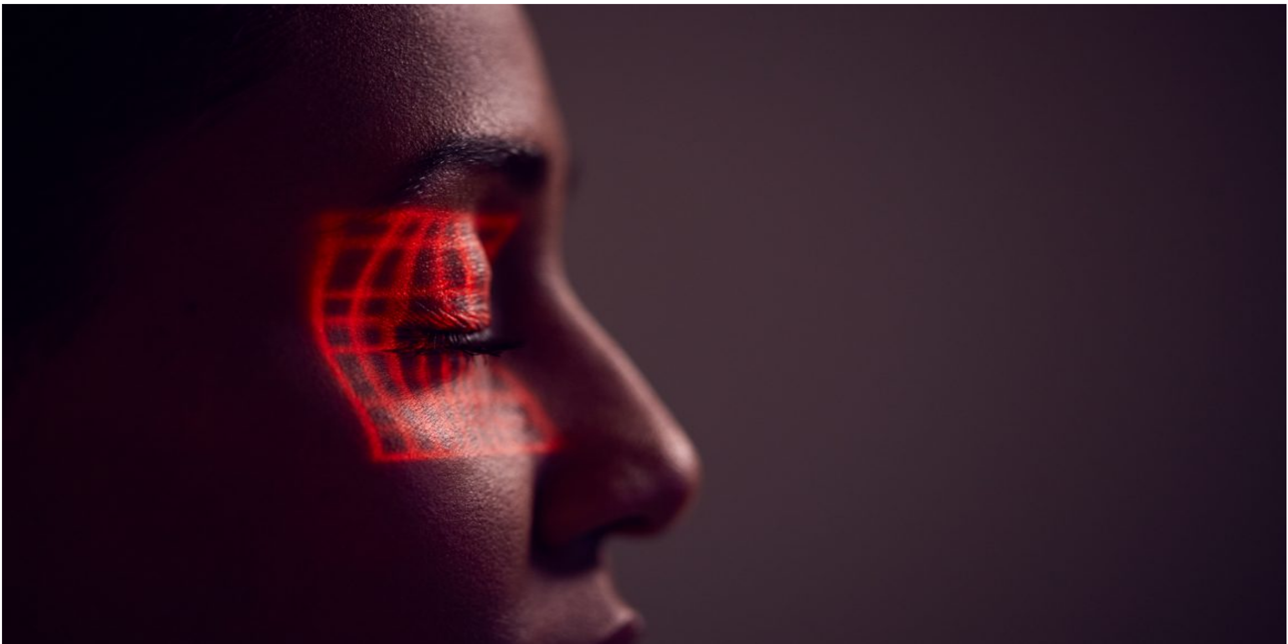
Hoe gezichtsherkenning van onschuldige burgers criminelen maakt

Nederland gebruikt speciale software om onschuldige burgers van fraude te beschuldigen en de EU spoort met gezichtsherkenning 'liegende reizigers' op. Zulke systemen worden verleden tijd, als het aan de Europese privacywaakhonden ligt.

-  Daan Bauwens

Leestijd: 9 minuten



Beeld door: monkeybusinessimages / iStock

Gezichtsherkenning in de openbare ruimte, in welke vorm dan ook, moet verboden worden. Dat adviseert het European Data Protection Board (EDPB), de koepel van privacytoezichthouders, aan de Europese Commissie. Daarnaast vindt het EDPB dat er een Europees verbod moet komen op kunstmatige intelligentie die mensen indeelt op basis van etniciteit, geslacht of seksuele geaardheid. De wetgeving die de Commissie in april voorstelde, gaat volgens de toezichthouders nog lang niet ver genoeg.

In de toeslagenaffaire, waarover de Nederlandse regering in januari viel, werden naar schatting 26.000 ouders slachtoffer van onterechte fraudeverdenkingen met de toeslag voor kinderopvang. De Systeem Risico-indicatiesoftware of SyRI koppelde gegevens uit verschillende overheidsdatabanken aan elkaar om te voorspellen of iemand al dan niet een fraudeur was. Mensen met een dubbele nationaliteit of met een 'exotische' familienaam werden extra gecontroleerd, net

als personen die in armere wijken woonden. Maar op dat soort AI, dat mensen indeelt op basis van geslachtskenmerken of huidskleur, moet als het aan de EDPB ligt dus een verbod komen, omdat het discriminatie in de hand werkt.

Terug naar de Victoriaanse tijd

Hoe de risicoberekening er in de toeslagenaffaire precies uitzag, werd nooit gedeeld. “Duidelijk was dat mensen geviseerd werden op basis van afkomst en postcode”, vertelt Ella Jakubowska van de Europese organisatie voor de verdediging van digitale rechten, EDRi. “Er wordt volgehouden dat dit geen aanslag is op onze basisrechten. Terwijl deze futuristische systemen ons in feite terug katapulteren naar de Victoriaanse tijd. Op basis van de afstand tussen je ogen of de grootte van je schedel werd toen bepaald of je een crimineel karakter had.”

Jakubowska heeft zelf een achtergrond als onderzoekster in een datalab van een tech-multinational. Ze liet zich als activiste inspireren door de vijf Amerikaanse steden die gezichtsherkenning in de publieke ruimte verboden hebben: Oakland, Somerville, Berkeley, Portland en San Francisco, de thuisbasis van Silicon Valley.

“

Gezichtsherkenning is ‘een oplossing op zoek naar een probleem’

Jakubowska wil een stap verder gaan en de Europese Commissie via een burgerinitiatief vragen om een verbod op elke vorm van biometrisch massatoezicht, inclusief gezichtsherkenning. “Wanneer is het gebruik van technologie echt noodzakelijk, legitiem en met wederzijdse instemming, in plaats van sexy en opwindend?” vraagt ze.

Maakt haar initiatief kans op slagen? Wojciech Wiewiórowski, de Europese Toezichthouder voor gegevensbescherming, stelde eind 2019 nog dat gezichtsherkenning ‘een symptoom van stijgende populistische intolerantie’ is en volgens hem ‘een oplossing op zoek naar een probleem’. Er is geen wetenschappelijk bewijs dat gezichtsherkenning een effect heeft op misdaad. De enige studie waar sprake was van een verband, toonde een marginaal effect op kruimeldiefstallen in parkeergarages, uitsluitend met bewakingscamera’s en zonder gezichtsherkenning.

Als in een sciencefictionfilm

Toch besluiten steeds meer politiekorpsen en overheden in Europa om de technologie uit te rollen. Nice in Zuid-Frankrijk is momenteel de koploper met 2600 camera’s, één per 128 inwoners. “Overheden gedragen zich in het beste geval naïef”, zegt Jakubowska. “Ze geloven het argument van techbedrijven dat dit een pasklare oplossing is tegen terrorisme of mensenhandel. Terwijl daar geen bewijzen voor zijn. Overheden in Europa zijn ook steeds vaker ondergefinancierd. Een cadeau van de steenrijke techindustrie is dus welkom, zeker als daarmee de schijn gecreëerd wordt dat de straten er veiliger op worden.”

De mogelijkheden voor onderdrukking en staatscontrole worden ondertussen alleen maar groter. Wie zal niet twee keer nadenken voor hij meedoet aan een protest in een publieke ruimte waar je gezicht geregistreerd kan worden? Dat heet in jargon het *chilling effect* en is volgens activisten een flagrante schending van het recht op vrije meningsuiting. “Zag je ooit een sciencefictionfilm

waarbij de overheid ons voortdurend in de gaten houdt, altijd weet waar we zijn, wie we zijn en wat we doen, en dat we daar dan met zijn allen beter van worden?” vraagt Jakubowska,

> “
>
> Kunnen we toelaten dat algoritmes beslissingen nemen over onze rechten?

En inderdaad, denk maar aan de filmklassieker Blade Runner (1982). In een van de meest iconische scènes van de film leggen verdachten de ‘Voight-Kampff-test’ af, een test die in het toen nog toekomstige jaar 2019 door de politie van Los Angeles in gebruik genomen zou worden, en op basis van biometrische gegevens – ademhaling, hartslag en kleur van het gelaat – zou uitmaken of iemand een gewone sterveling was of een genetisch gemodificeerde replica.

Was de film wellicht een inspiratiebron voor de Europese Commissie? In elk geval liep de timing van haar iBorder-Ctrl-systeem akelig synchroon: in 2019 liepen de experimenten daarmee af. iBorderCtrl is een geautomatiseerd systeem aan de buitengrenzen van de EU dat uitmaakt of inreizende personen al dan niet liegen, op basis van microbewegingen in het gezicht. Wie verdacht wordt van liegen, wordt strenger gecontroleerd door de grensagenten. Zo zouden illegale migranten en terroristen onderschept worden, aldus de Europese Commissie.

De Commissie investeerde 4,5 miljoen euro in het project. Ze weigerde het evaluatierapport in 2019 openbaar te maken; dat zou de commerciële belangen van de bedrijven achter het project kunnen schaden. Duits Europarlementslid Patrick Breyer van de Duitse Piratenpartij deed het project stellig af als ‘pseudowetenschappelijke veiligheidshocuspocus’. Hij daagde de Commissie voor het Europees Hof van Justitie omdat die het rapport niet publiek wil maken. De eerste zitting vond plaats op 5 februari, de uitspraak moet nog volgen.

De vraag die Breyers rechtszaak in essentie stelt is de volgende: kunnen we toelaten dat bedrijven algoritmes ontwikkelen die beslissingen nemen over onze rechten, terwijl we niet mogen weten waarop die beslissingen gebaseerd zijn? En houden overheden nog wel voldoende het publieke belang voor ogen, of laten zij zich voor het karretje spannen van de techbedrijven?

Het grootste identificatiesysteem ter wereld

Wie wil weten welke gevolgen zulke algoritmes kunnen hebben, hoeft maar naar India te kijken. Daar kunnen burgers een twaalfcijferige code krijgen, in ruil voor hun naam, geboortedatum, gender, adres, een pasfoto, tien vingerafdrukken en een irisscan. Die code stelt Indiërs in staat om vlot aan uitkeringen, voedselhulp of pensioenen te komen. De identiteitscode valt onder het project Aadhaar, Hindi voor ‘fundament’, dat in 2009 van start ging. Biometrische dataverzameling, het digitaal opslaan van meetbare, kenmerkende biologische eigenschappen van individuen zoals vingerafdrukken of gezichtsfoto’s, wordt nergens zo massaal uitgerold als in India.

Registratie zou vrijwillig moeten zijn, maar de Indiase overheid maakt steeds meer uitkeringen en diensten afhankelijk van het hebben van een Aadhaar-nummer. Aadhaar bevat intussen de biometrische gegevens van 1,26 miljard Indiërs en is daarmee het grootste biometrische identificatiesysteem ter wereld. Maar het is beslist niet het enige.

> “
>
> In de kleine lettertjes wordt om toegang gevraagd tot je persoonlijke gegevens

De Unique Identification Authority of India of UIDAI is het centrale orgaan dat verantwoordelijk is voor het management van Aadhaar. Het hield tijdens rechtszaken in het Hooggerechtshof steeds vol dat het gaat om een geanonimiseerd systeem, waarin de privacy van gebruikers verregaand wordt beschermd. Maar dat blijkt niet te kloppen. Er is een wetgevend kader voor de biometrische databank, de Aadhaar Act, en die gaat het verst in de bescherming van je biometrische gegevens, dus alle biologische informatie behalve de gezichtsfoto.

Maar de wet beschermt niet de identiteitsgegevens die aan de twaalfcijferige code verbonden zijn: naam, adres, geboortedatum, telefoonnummer. Volgens sectie 8 van de wet mogen die gegevens aan 'verzoekende partijen' doorgegeven worden. Met andere woorden: als een telecombedrijf je vingerafdrukken en Aadhaar-nummer vraagt bij de aankoop van een simkaart, krijgt het op verzoek toegang tot al je persoonlijke informatie.

Gebrek aan transparantie

Sectie 8 voorziet wel een kleine bepaling voor de bescherming van die persoonlijke informatie: een verzoekende partij mag je persoonlijke informatie pas gebruiken als je daarvoor toestemming geeft. Critici geven echter aan dat die toestemming vaak in de kleine lettertjes van een pop-upscherm staat, dat je ziet wanneer je je verplicht registreert voor een nieuwe simkaart of voor de aankoop van bijvoorbeeld een koelkast.

Er is nog een uitzondering: op grond van 'nationale veiligheidsredenen' kan de overheid alle identiteitsgegevens inzien. De wet geeft geen specifieke invulling van die term 'nationale veiligheidsredenen'. Met andere woorden: bedrijven en de overheid kunnen gemakkelijk bij alle persoonlijke gegevens gekoppeld aan het Aadhaar-nummer. Telecomreus Reliance Jio heeft al persoonlijke dossiers van 100 miljoen Indiërs aangelegd met informatie uit het Aadhaar-systeem. Het leent zich erg goed voor datamining, doorgedreven gegevensanalyse door bedrijven.

> “
>
> Mensen kwamen om van de honger doordat ze door een systeemfout geen voedselsteun kregen

Techbedrijf Infosys ontwierp het systeem voor de overheid en richtte de UIDAI op, en CEO Nandan Nilekani blijft tot op de dag van vandaag volhouden dat het slechts om een identificatiesysteem gaat. Tegelijk klopt India zichzelf op de borst omdat het als eerste land zijn nationale databank openstelde voor private ondernemers en daarmee 'ongekende innovatie' mogelijk maakte.

Ondanks de goednieuwsshow van de Indiase overheden en techbedrijven worden hele lagen van de Indiase maatschappij hard getroffen door Aadhaar. En niet alleen door voor de hand liggende privacykwesties. Het systeem, dat oorspronkelijk bedacht was om fraude met overheidssteun tegen te gaan en ongedocumenteerde migranten het land uit te jagen, laat het soms simpelweg afweten. Vingerafdrukken worden niet herkend, ambtenaren weigeren assistentie en het internetbereik in India is op veel plekken te zwak om het systeem altijd draaiend te houden.

Dodelijke systeemfouten

Dat kan fatale gevolgen hebben, vooral als staten slordig omspringen met die databanken. Zo waren de zwangerschapsdata van zo'n twee miljoen mensen uit deelstaat Andhra Pradesh terug te vinden op de overheidswebsite, inclusief de naam van de vader en of ze een abortus hadden laten uitvoeren.

Vrouwenrechtenactivisten wijzen erop dat dit soort datalekken mensen aanzet om buiten het reguliere gezondheidscircuit naar hulp te zoeken. Ook een artikel in het British Medical Journal van 2017 bespreekt de gevaren van Aadhaar voor de gezondheid van mensen, en vrouwen in het bijzonder. Zo zijn er gevallen bekend van mensen die hulp geweigerd wordt omdat ze geen Aadhaar-nummer willen voorleggen. In Chandigarh liet een bediende bijna het leven na een amateuristisch uitgevoerde abortus. Het staatshospitaal had de vrouw geweigerd omdat ze niet wilde dat haar Aadhaar-nummer geregistreerd werd.

Er was ook sprake van om de overheidssteun voor sekswerkers tijdens de coronacrisis afhankelijk te maken van het voorleggen van een Aadhaar-nummer. Maar de oudste beweging voor sekswerkers van het land wist het Hooggerechtshof ervan te overtuigen dat niet toe te laten. Hun recht op anonimiteit bleef behouden. Geregistreerd staan als sekswerker in een databank van de overheid kan ernstige gevolgen hebben. In India is het verstrekken van financiële diensten aan sekswerkers bij wet verboden. En banken blijken via de Aadhaar-nummers ook vaak toegang te hebben tot overheidsdatabanken.

> "
>
> Hoe neutraal is technologie als politiediensten en ministeries weten wie hindoe is en wie moslim?

India lijkt intussen klaar voor een nieuw hoofdstuk in de biometrische registratie van haar burgers: er staat een project in de steigers voor de uitrol van een nationaal systeem van gezichtsherkenning via bewakingscamera's. Het systeem heeft nog geen naam, maar komt onder de controle te staan van het ministerie van Binnenlandse Zaken. De gegevens zullen toegankelijk zijn voor elk politiekantoor in India.

New Delhi kreeg een jaar geleden al een voorproefje van wat dat zou kunnen betekenen. Minister van Binnenlandse Zaken Amit Shah vertelde toen aan het Indiase parlement dat 1100 relschoppers waren geïdentificeerd via gezichtsherkenning tijdens rellen in New Delhi. Die braken uit in de nasleep van de omstreden 'Burgerschapswet' waarmee religieuze minderheden uit Bangladesh, Pakistan en Afghanistan de Indiase nationaliteit kunnen verwerven, maar moslims zijn uitgesloten van de procedure.

'Software ziet geen religie'

Daardoor leek het alsof moslims de rellen waren begonnen. Maar in onafhankelijke rapporten stond dat juist moslimwijken het doelwit waren van gerichte aanvallen door nationalistische hindoes. Minister Shah houdt vol dat AI neutraal is. 'Dit is software. Die ziet geen religie, geen klederdracht. Hij ziet enkel het gezicht en zo worden de daders gepakt.'

Maar er is alle reden om te twijfelen aan die neutraliteit. Hoe neutraal is de technologie als politiediensten en ministeries weten wie hindoe is en wie moslim? Shah gaf namelijk toe dat data van gezichtsherkenning vergeleken werden met beelden uit databanken in het bezit van de overheid,

zoals identiteitskaarten, rijbewijzen en ‘andere databanken’. Software ziet misschien geen religie, maar Aadhaar en de hindoe-nationalistische minister Shah wel.

> “
>
> Ondanks internationale kritiek zet India zichzelf in de markt als dé techbestemming van Azië

Anushka Jain, een jonge vrouw uit New Delhi, leidt het project Panoptic, dat technologie voor gezichtsherkenning in kaart brengt voor de Internet Freedom Foundation (IFF), een vereniging voor de bescherming van digitale rechten in New Delhi. Ze verwijt de Indiase overheid gebrek aan transparantie, en de uitoefening van politieke controle toegedekt door de voorgewende neutraliteit van technologie. “Hoe kun je anders verklaren dat juist die groepen die het meest gediscrimineerd zijn ook het vaakst het slachtoffer worden van deze technologie?”

Vrouwen, bijvoorbeeld. Jain vertelt over de stad Lucknow in Uttar Pradesh, waar de politie plannen aankondigde voor een bewakingssysteem met gezichtsherkenning. “In wijken waar veel vrouwen passeren en waar vrouwen vaak worden lastiggevallen door mannen”, zegt Jain, “zouden intelligente camera’s in staat zijn om de gezichtsexpressie van vrouwen te lezen. Zodat in het geval van emotionele stress een alarm afgaat in het dichtstbijzijnde politiestation. Dat lijkt misschien een goed idee, maar ik kan me persoonlijk geen grotere inbreuk op mijn privacy bedenken.” India is berucht om zijn bijzonder slechte staat van dienst als het gaat om seksueel grensoverschrijdend gedrag, ook bij politiekorpsen.

De internationale kritiek op Aadhaar en gezichtsherkenning ten spijt, zet India zich bewust in de markt als dé nieuwe tech-bestemming in Azië. Niet *ondanks*, maar *dankzij* de vrije beschikbaarheid van persoonlijke gegevens. Want data is immers de nieuwe olie.

Een eerdere versie van dit artikel verscheen op MO en op OneWorld op 15 april 2021.*